THE O'MARA LAW FIRM, P.C.
David C. O'Mara
311 East Liberty St.
Reno, Nevada 89501
Tel: 775-323-1321
Fax: 775-323-4082
Email: david@omaralaw.net

FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
Todd S. Garber, Esq.*
Andrew C. White, Esq.*
One North Broadway, Suite 900
White Plains, New York 10601
Tel: (312)621.2000

*pro hac vice forthcoming

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

CRYSTAL BREWSTER, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CAESARS ENTERTAINMENT, INC.,

Defendants.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Crystal Brewster ("Plaintiff"), on behalf of herself and all others similarly situated ("Class Members"), file this Class Action Complaint ("Complaint") against Defendant Caesars Entertainment, Inc. ("Caesars" or "Defendant"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Caesars for its failure to safeguard and secure the personally identifiable information ("PII") of past and current customers of Defendant, including Plaintiff. The individuals affected are past and current customers of Caesars, whose PII was within Caesars' loyalty program database.

2. The data reportedly exposed in the breach includes some of the most sensitive types of data that cybercriminals seek in order to commit fraud and identity theft. According to Caesars, information disclosed in the breach includes, but is not limited to, their names, mailing addresses, telephone numbers, email addresses, dates of birth, driver's license numbers, and Social Security Numbers, for a "significant number" of its more than 65 million members of its loyalty program.[1]

3. Caesars' is a global hospitality and gaming company with its principal place of business in Reno, Nevada. Caesars joined with Eldorado Resorts to "create the largest and most diversified collection of destinations across the U.S." It consists of "over 50 world-class resorts" and its loyalty program is the "[first] and largest loyalty program in the industry[.]"[2]

---

[1] According to Defendant's Form 8-K filing with the SEC on September 14, 2023, "[O]n September 7, 2023, we determined that the unauthorized actor acquired a copy of, among other data, our loyalty program database, which includes driver's license numbers and/or social security numbers for a significant number of members in the database." SEC Form 8-K, Caesars Entertainment, Inc., Sept. 14, 2023, available at: https://www.sec.gov/ix?doc=/Archives/edgar/data/0001590895/000119312523235015/d537840d8k.htm (last visited Oct. 25, 2023).

[2] Corporate, Caesars, https://www.caesars.com/corporate (last visited Oct. 25, 2023).

4. On or about September 7, 2023, Caesars determined that a malicious actor had gained access to its network systems and accessed the PII of Plaintiff and Class members (the "Data Breach").[3]

5. Armed with the Personal Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial information in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, and using Class members' health information to target other phishing and hacking intrusions based on their individual.

6. As a result of the Data Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of medical and financial fraud and identity theft. Plaintiff and Class members must now and in the future closely monitor their financial accounts and medical information to guard against identity theft.

7. Caesars owed a non-delegable duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure.[4] Caesars breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its customers' PII from unauthorized access and disclosure.

8. As a result of Caesars' inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of

---

[3] Caesars' Oct. 6 Filing with the Maine Attorney General reports that the Data Breach originated from a social engineering attack on Caesars' outside IT vendor, which allowed the hackers access to the loyalty program database. Caesars' Filing, Maine Attorney General, available at: https://www.sec.gov/ix?doc=/Archives/edgar/data/0001590895/000119312523235015/d537840d8k.htm (last visited Oct. 25, 2023).

[4] Caesars also understood the need to safeguard the PII it collects and maintains for its financial benefit, as reflected by its Privacy Policy posted on its website, which represents that: "We maintain physical, electronic, and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control." Privacy Policy, Caesars, https://www.caesars.com/corporate/privacy (last visited Oct. 25, 2023).

herself and all persons whose PII was exposed as a result of the Data Breach, which Caesars learned of on or about September 7, 2023, and first publicly acknowledged on September 17, 2023.

9. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendants' data security system, future annual audits, and adequate credit monitoring services funded by Defendants.

10. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

11. Plaintiff Crystal Brewster is a New York resident. On October 14, 2023, Plaintiff Brewster received a letter from Caesars notifying her that her PII was among the information accessed by cybercriminals in the Data Breach.[5]

12. Plaintiff Brewster has been a member of the Caesars' Reward program since May 31, 2014, which is over nine years ago. She attended and used her Caesars' Rewards membership at Caesars' Atlantic City in May 2014, June 2016, July 2020, and April 2021, and she has stayed at that Caesars' property on at least one occasion.

13. Plaintiff Brewster has suffered injuries directly and proximately caused by the Data Breach. These include, but are not limited to, loss of time and money expended to mitigate the imminent and significant risk of identity theft, loss of privacy, and anxiety and other emotional distress. Specifically, Plaintiff Brewster has purchased and enrolled in multiple identity theft protection services, which notified her that her information was on the "dark web." Plaintiff Brewster has received multiple notifications of unauthorized credit inquiries, which negatively

[5] At the time of, and reflected in, the Incident Notice letter Plaintiff Brewster received on October 19, 2023, Plaintiff Crystal Brewster was previously known as Sequann Brewster. As of March 14, 2021, per a Certified Order of NYC Civil Court, Queens County, she was authorized to assume her current name of Crystal Brewster.

affected her credit score. Plaintiff Brewster also changed all her passwords and obtained new credit cards.

14. Had Plaintiff Brewster known that Caesars would not adequately protect her and Class members' PII, she would not have received services from Caesars and would not have provided her PII to Caesars.

15. Defendant Caesars Entertainment, Inc. is a publicly traded company incorporated in the State of Delaware and has its principal place of business at 100 West Liberty Street, 12th Floor, Reno, NV 99501.

16. Caesars owns, operates, and manages hotels, casinos, and resorts located predominantly in Nevada. Caesars' Las Vegas property portfolio includes Caesars' Place Las Vegas, The Cromwell, Flamingo Las Vegas, Horseshoe Las Vegas, The LINQ Hotel & Casino, Paris Las Vegas, Planet Hollywood Resort & Casino, Harrah's Las Vegas, and Rio All-Suite and Casino.[6]

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interests and costs.

18. This Court has diversity jurisdiction over Plaintiff's claims pursuant to 29 U.S.C. § 1332(a)(1) because Plaintiff and Defendant are citizens of different states and the amount in controversy exceeds $75,000.

19. This Court has general personal jurisdiction over Caesars because Caesars maintains its principal place of business in Nevada. This Court also has specific personal jurisdiction over Caesars because Caesars engaged in the conduct underlying this action in Nevada, including the collection, storage, and inadequate safeguarding of Plaintiff's and Class members' PII.

---

[6] *See* Caesars Entertainment, Inc. Form 10-K for 2022, at pg. 28, available at: https://investor.caesars.com/static-files/abff6ce9-34b1-4057-9c78-db6bf146c295 (last visited Oct. 25, 2023).

20. Venue in proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Within this District, Caesars maintains its principal place of business, entered into consumer transactions with Plaintiff, and made its data security decisions leading to the Data Breach.

FACTUAL ALLEGATIONS

Overview of Caesars

21. Caesars is a global hospitality and gaming company. The company provides amenities and services such as restaurants, entertainment, meeting and conventions facilities, and shopping.[7]

22. In the regular course of its business, Caesars collects and maintains the PII of its loyalty rewards program members.

23. Plaintiff and Class members are, or were, loyalty rewards program members of Caesars, and entrusted Caesars with their PII.

The Data Breach

24. On or about September 7, 2023, Caesars discovered that unauthorized users had gained access to its loyalty reward program's network systems.

25. On or about September 14, 2023, Caesars filed a Form 8-K with the SEC in which Caesars disclosed that it had bene the target of a cyberattack that led to the Data Breach.[8]

26. Around the same time as the filing of the Form 8-K, Caesars published a similar statement on its Informational Website, informing the public that a social engineering attack on one of its outsourced IT support vendors had led to an unauthorized actor acquiring a copy of Caesars' loyalty program database, "which includes driver's license numbers and/or social security numbers for a significant amount of members in the database."[9]

---

[7] Corporate, *supra* note 2.

[8] SEC Form 8-K, *supra* note 1.

[9] *See* Caesars Informational Website, Learn More, available at: https://response.idx.us/caesars/#learn-more (last visited Oct. 25, 2023).

27. To date, Caesars has not disclosed crucial information, including, but not limited to: how many of its loyalty rewards program members were affected by the Data Breach; how the cybercriminals were able to exploit vulnerabilities in Caesars' IT security systems; the identity of Caesars' outsourced IT vendor; the identity of the hacking group responsible for the Data Breach; or steps Caesars has taken to ensure that such an attack does not occur again.

28. News organizations have identified Scattered Spider, also known as UNC 3944, a group specializing in social engineering attacks, to be responsible for the Data Breach.[10] Reportedly, Caesars paid approximately $15 million in ransom to the hackers to ensure that the data was not leaked.[11]

29. While Caesars has not disclosed the exact data obtained in the data breach, upon information and belief, the data likely consists of PII including, but not limited to, names, addresses, email addresses, and dates of birth, as well as driver's license numbers and Social Security numbers.

Caesars Knew That Criminals Target PII

30. At all relevant times, Caesars knew, or should have known, its loyalty reward members' Plaintiff's, and all other Class members' PII was a target for malicious actors.[12] Despite such knowledge, Caesars failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that Caesars should have anticipated and guarded against.

31. Caesars' data security obligations are and were particularly important given the substantial increase in cyberattacks and/or data breaches widely reported on in the last few years. In

---

[10] *See e.g.*, Zack Whittaker, *Caesars Entertainment says customer data stolen in cyberattack*, TechCrunch (Sept. 14, 2023, 9:40 AM), https://techcrunch.com/2023/09/14/caesars-entertainment-data-breach-cyberattack/.

[11] *Id.*

[12] *See* Privacy Policy, *supra* note 4.

fact, in the wake of this rise in data breaches, the Federal Trade Commission has issued an abundance of guidance for companies and institutions that maintain individuals' PII.[13]

32. PII is a valuable property right.[14] The value of PII is a commodity is measurable.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[17] In fact, it is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[13] *See, e.g., Protecting Personal Information: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Oct. 25, 2023).

[14] See Marc van Lieshout, The Value of Personal Data, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[15] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[16] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[17] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

33. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

34. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[18]

35. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

36. Therefore, Caesars clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place.

Theft of PII has Grave and Lasting Consequences for Victims

37. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victims' name, lock the victim out of his or her financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[19]

---

[18] Janice Y. Tsai, et al., The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[19] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

38. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[20] In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[21]

39. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact to their credit.

40. Indeed, Plaintiff Brewster appears to have already been the victim of attempted bank fraud following the Data Breach, which cost her time to address and affected her credit rating.

41. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[22] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

---

[20] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FRC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[21] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Oct. 25, 2023).

[22] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, United States Government Accountability Office (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Oct. 25, 2023).

42. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[23]

43. There may be a time lag between when PII is stolen and when it is used.[24] According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

44. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security Numbers, and other PII directly on various Internet websites making the information publicly available.

45. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is

---

[23] *Id.* at 2, 9.

[24] For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information. John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf.

[25] *Id.* at 29 (emphasis added).

employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[26]

46. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft, and some need over a year.[27]

47. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

48. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (v) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

49. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

50. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

---

[26] Patrick Lucas Austin, *'It is Absurd.' Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[27] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RESOURCE CENTER, https://www.idthecenter.org/identity-theft-aftermath-study/ (last visited Nov. 4, 2022).

> All persons whose PII was accessed in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

51. Plaintiff reserves the right to amend the above definition, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

52. Plaintiff is a member of the Class.

53. Excluded from the Class is Caesars Entertainment, Inc. and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

54. This action seeks both injunctive relief and damages.

55. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

56. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of Class members is unknown at this time, Class members are readily identifiable in Caesars' records, which will be a subject of discovery. Upon information and belief, there are millions of Class members in the Class.

57. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Caesars' data security systems prior to the Data Breach met the requirements of relevant laws;
b. Whether Caesars' data security systems prior to the Data Breach met industry standards;
c. Whether Caesars owed a duty to Plaintiff and Class members to safeguard their PII;
d. Whether Caesars breached its duty to Plaintiff and Class members to safeguard their PII;
e. Whether Caesars failed to provide timely and adequate notice of the Data Breach to Plaintiff and Class members;
f. Whether Plaintiff's and Class members' PII was compromised in the Data Breach;
g. Whether Plaintiff and Class members are entitled to injunctive relief; and
h. Whether Plaintiff and Class members are entitled to damages as a result of Caesars' conduct.

58. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same

violations of law. Plaintiff and Class members all had their PII stolen in the Data Breach. Plaintiff's grievances, like the proposed Class members' grievances, all arise out of the same business practices and course of conduct by Caesar.

59. **Adequacy of Representation.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. Her interests do not conflict with the interests of the Class.

60. Plaintiff and her chosen attorneys -- Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG") and The O'Mara Law Firm, P.C. -- are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint.

61. FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. FBFG's attorneys are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class members. Finally, FBFG possesses the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

62. **Predominance.** The common issues identified above arising from Caesars' conduct predominate over any issues affecting only individual Class members. The common issues hinge on Caesars' common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

63. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large a number of injured persons, to keep the courts from becoming paralyzed by hundreds -- if not thousands -- of repetitive cases, and to reduce transaction costs so that the injured Class members can obtain the most compensation possible.

64. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in

the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Syracuse University students, alumni, and applicants, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class members can be identified from Defendant's records, such that direct notice to the Class members would be appropriate.

65. **Injunctive relief.** Caesars has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

CAUSES OF ACTION
COUNT I
NEGLIGENCE

66. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

67. As a condition of receiving Caesars' services, Plaintiff and Class members were required to provide Caesars with their PII.

68. Caesars knew the risks of collecting and storing Plaintiff's and all other Class members' PII and the importance of maintaining secure systems. Caesars knew of the many data breaches that targeted companies that store PII in recent years.

69. Caesars owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

70. Caesars' duty of care arose from, among other things:

a. the special relationship that existed between Caesars and its customers, as only Caesars was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Class from the Data Breach.
b. Section A of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.
c. Caesars' representations in its Privacy Policy;
d. Industry standards for the protection of confidential information
e. General common law duties to adopt reasonable data security measures to protect customer PII and to act a reasonable and prudent person under the same or similar circumstances would act; and
f. State statutes requiring reasonable data security measures, including, but not limited to, Nev. R. Stat. § 603A.210, which states that business possessing personal information of Nevada residents "shall implement and maintain reasonable security measures to protect those records from authorized access."

71. Plaintiff and Class members provided and entrusted their PII to Caesars with the understanding that Caesars would take reasonable measures to safeguard their information.

72. Given the sensitivity and value of the PII Caesars collected, and the extensive resources at its disposal, Caesars should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

73. Defendant breached its common law, statutory, and other duties -- and thus, was negligent -- by failing to use reasonable measures to protect Plaintiff's and Class members' PII, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and the Class members' PII;
b. failing to adequately monitor the security of its networks and systems;
c. allowing unauthorized access to Plaintiff's and the Class members' PII; and
d. failing to warn Plaintiff and other Class members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

74. Caesars' violations of the FTCA and state data security statutes constitute negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from the Data Breach.

75. Caesars owed a duty of care to the Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

76. It was foreseeable that Caesars' failure to use reasonable measures to protect PII and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

77. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

78. Caesars knew or reasonably should have known of the inherent risks in collecting and storing the PII of Plaintiff and members of the Class and the critical importance of providing adequate security of that information, yet despite the foregoing had inadequate cyber-security systems and protocols in place to secure the PII.

79. As a result of the foregoing, Caesars unlawfully breached its duty to use reasonable care to protect and secure the PII of Plaintiff and the Class which Plaintiff and members of the Class were required to provide to Caesars as a condition of enrollment in its loyalty rewards program.

80. Plaintiff and members of the Class reasonably relied on Caesars to safeguard their information, and while Caesars was in an exclusive position to protect against harm from a data breach, Caesars negligently and carelessly squandered that opportunity. As a proximate result, Plaintiff and members of the Class suffered and continue to suffer the consequences of the Data Breach.

81. Caesars' negligence was the proximate cause of harm to Plaintiff and members of the Class.

82. Had Caesars not failed to implement and maintain adequate security measures to protect the PII of its consumers, Plaintiff's and Class members' PII would not have been exposed to unauthorized access and stolen, and they would not have suffered any harm.

83. As a direct and proximate result of Caesars' negligence, Plaintiff and members of the Class have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiff and members of the Class have been injured by, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) the improper compromise, publication, and theft of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

84. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

COUNT II
NEGLIGENCE PER SE

85. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

86. Caesars' duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Caesars, of failing to employ reasonable measures to protect and secure PII.

87. Caesars' duties also arise from Nev. R. Stat. § 603A.210, which states that business possessing personal information of Nevada residents "shall implement and maintain reasonable security measures to protect those records from authorized access."

88. Caesars violated Section 5 of the FTCA and Nev. R. Stat. § 603A.210 by failing to use reasonable measures to protect Plaintiff's and all Class members' PII and not complying with applicable industry standards. Caesars' conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII, including, specifically, the substantial damages that would result to Plaintiff and other Class members.

89. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA and Nev. R. Stat. § 603A.210 were intended to guard against.

90. It was reasonable foreseeable to Caesars that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

91. The injury and harm that Plaintiff and Class members suffered was the direct and proximate result of Caesars' violations of Section 5 of the FTCA and Nev. R. Stat. § 603A.210. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) the improper compromise, publication, and theft of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

92. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

COUNT III
BREACH OF FIDUCIARY DUTY

93. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

94. Plaintiff and Class members gave Caesars their PII in confidence, believing that Caesars would protect that information. Plaintiff and Class members would not have provided Caesars with this information had they known it would not be adequately protected. Caesars' acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between Caesars and Plaintiff and Class members. In light of this relationship, Caesars must act primarily for the benefit of its loyalty rewards program members, which includes safeguarding and protecting Plaintiff's and Class members' PII.

95. Caesars has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII and otherwise failing to safeguard Plaintiff's and Class members' PII that it collected.

96. As a direct and proximate result of Caesars' breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) the improper compromise, publication, and theft of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (v) the continued risk to their PII which remains in Caesars' possession; and (vi) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

97. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

98. Caesars required Plaintiff and Class members to provide their PII in order to use Caesars' services. Specifically, Caesars requires consumers to provide their PII during the

reservation and/or check-in process, as well as the online process for creating a loyalty rewards account. By virtue of accepting Plaintiff's PII in these processes, Caesars implicitly represented that its data security systems were reasonably sufficient to safeguard the PII.

99. Plaintiff and Class members entrusted their PII to Caesars, and in so doing, they entered into implied contracts with Caesars.

100. Pursuant to these implied contracts, in exchange for the consideration and PII provided by Plaintiff and Class members, Caesars agreed to, among other things, and Plaintiff understood that Caesars would: (1) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; (2) protect Plaintiff's and Class members' PII in compliance with federal and state laws and regulations and industry standards.

101. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Caesars, on the other hand. Indeed, as set forth *supra*, Caesars recognized its duty to provide adequate data security and ensure the privacy of its consumers' PII with its practice of providing a privacy policy on its website.[28] Had Plaintiff and Class members known that Caesars would not adequately protect its consumers' PII, they would not have received services from Caesars.

102. Plaintiff and Class members performed their obligations under the implied contract when they provided Caesars with their PII and paid for the services from Caesars.

103. Caesars breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

104. Caesars' breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

---

[28] *See* Privacy Policy, *supra* note 4.

105. Plaintiff and all other Class members were suffered by Caesars' breach of implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

106. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

107. This claim is pleaded in the alternative to the breach of implied contract claim.

108. Plaintiff and Class members conferred a monetary benefit upon Caesars in the form of monies paid for services.

109. Caesars accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Caesars also benefitted from the receipt of Plaintiff's and Class members' PII, as this was used to facilitate payment. Additionally, Caesars used Plaintiff and Class members' PII for a variety of profit-generating purposes, as Caesars used the PII for marketing to generate future stays from consumers and derive future revenues and profit.

110. As a result of Caesars' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

111. Caesars should not be permitted to retain the money belonging to Plaintiff and Class members because Caesars failed to adequately implement the data privacy and security procedures

for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

112. Caesars should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VI
VIOLATION OF THE NEVADA CONSUMER FRAUD ACT
NEV. REV. STAT. § 41.600

113. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

114. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 states:

> 1. An action may be brought by any person who is a victim of consumer fraud.
> 2. As used in this section, "consumer fraud" means: . . . (e) A deceptive trade practice as defined in NRS 598.095 to 598.0925, inclusive.

115. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 598.0923(2) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 2) Fails to disclose a material fact in connection with the sale or lease of goods or services." Caesars engaged in a deceptive trade practice, as defined by this provision, because it failed to disclose the material fact that its data security systems and practices were deficient and inadequate to protect consumers' PII.

116. Caesars knew or should have known that its data security was deficient, especially considering its vast resources and the amount and types of PPI it collected from Plaintiff and Class members. Thus, Caesars had knowledge of facts that constituted the omission.

117. Caesars' inadequate data security was a material fact connected to the sale of its services because Caesars required Plaintiff and Class members to provide their PPI to receive its services, as explained in more detail above. Plaintiff and Class members would not have provided their PPI and/or paid for obtained Caesars' services had they known of Caesars' inadequate data security.

118. Caesars should and could have made a proper disclosure when selling its services, including in the registration for its Caesars' Rewards loyalty program, even if it did not require

payment at the time of registration, as such process and program are clearly in furtherance of the selling of Caesars' services.

119. Nev. Rev. Stat. § 598.0923(3) additionally defines a "deceptive trade practice" as when: "[I]n the course of his or her business or occupation[, a person] knowingly: . . . 3) Violates a state or federal statute or regulation relating to the sale or lease of . . . services." Caesars breached multiple statutes, each of which is an independently sufficient predicate act for purposes of establishing its violation of § 598.0923(3), and as follows, Nev. Rev. Stat. § 41.600. Caesars also knew or should have known that it violated each of these statutes.

120. *First,* Caesars breached Nev. Rev. Stat. § 603A.210(1), as alleged in further detail above, which requires: "A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain *reasonable security measures* to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." (Emphasis added).

121. Nev. Rev. Stat. § 603A.030 defines "data collector" as including "any . . . corporation, . . . or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information." Thus, Caesars is a data collector, subject to the requirements of Nev. Rev. Stat. § 603A.210(1).

122. *Second*, Caesars also violated Nev. Rev. Stat. § 59.0923(2), as alleged above in this Count.

123. *Third*, Caesars violated the FTC Act, 15 U.S.C. § 45, as alleged in Count II.

124. Caesars failed to implement and maintain reasonable security measures, evidenced by the occurrence and severity of this Data Breach.

125. Caesars' violations of these statutes were done knowingly, satisfying that requirement of 598.0923(3). Caesars knew or should have known that its data security practices were deficient, as explained in further detail above.

126. Plaintiff and Class members were denied a benefit conferred on them by the Nevada legislature.

127. Nev. Rev. Stat. § 41.600(3) states that if the plaintiff prevails, the court "shall award: (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court deems appropriate; and (c) the claimant's costs in the action and reasonable attorney's fees."

128. As a direct and proximate result of the foregoing, Plaintiff and Class members suffered all forms of damages alleged herein. Plaintiff's harms constitute compensable damages under Nev. Rev. Stat. § 41.600(3).

129. Plaintiff and Class members are also entitled to all forms of injunctive relief sought herein.

130. Plaintiff and Class members are also entitled to an award of their attorney's fees and costs.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Caesars as follows:

A. Certifying that Class as requested herein, appointing the named Plaintiff as Class representative and the undersigned counsel as Class counsel;

B. Requiring that Defendant pay for notifying the members of the Class of the pendency of this suit;

C. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

D. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Caesars from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend additional credit monitoring services and similar services to protect against all types of identity theft and medical identity theft.

E. Awarding Plaintiff and the Class prejudgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable, together with their costs and disbursements of this action; and

G. Awarding Plaintiff and the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: October 26, 2023

THE O'MARA LAW FIRM, P.C.

/s/ David C. O'Mara, Esq.

DAVID C. O'MARA, ESQ.
311 E. Liberty St
Reno, NV 89501
775.323.1321
david@omaralaw.net

FINKELSTEIN, BLANKINSHIP
FREI-PEARSON & GARBER, LLP
Todd S. Garber, Esq.*
Andrew C. White, Esq.*
One North Broadway, Suite 900
White Plains, New York 10601
Tel: (312)621.2000
tgarber@fbfglaw.com
awhite@fbfglaw.com
*pro hac vice forthcoming

Attorneys for Plaintiffs